Efficient and Secure Coordination Channels in the Access Grid

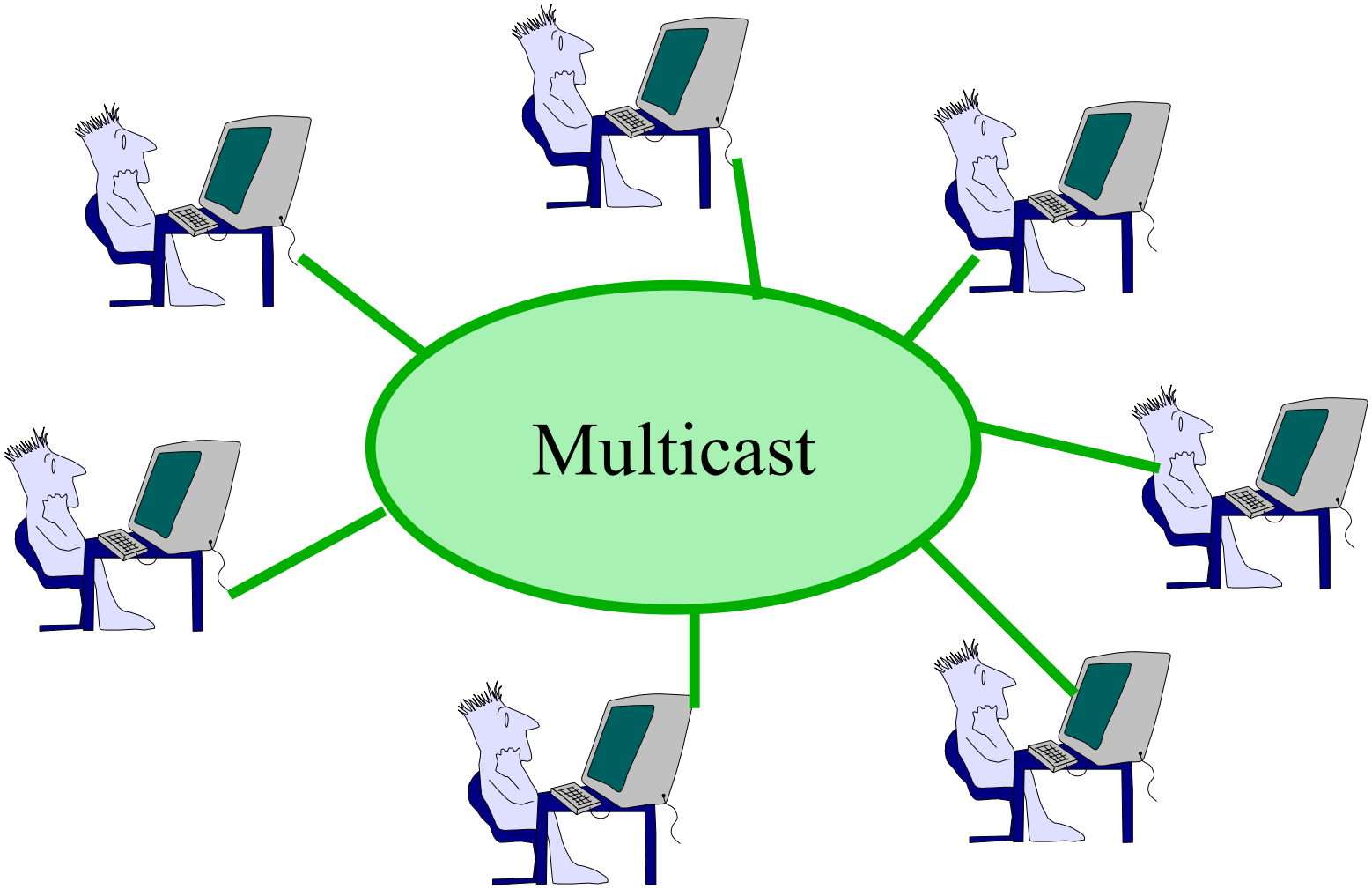
Deb Agarwal (DAAgarwal@lbl.gov)
Ernest Orlando Lawrence Berkeley National Laboratory
http://www-itg.lbl.gov/CIF/GroupComm/

Group Communication

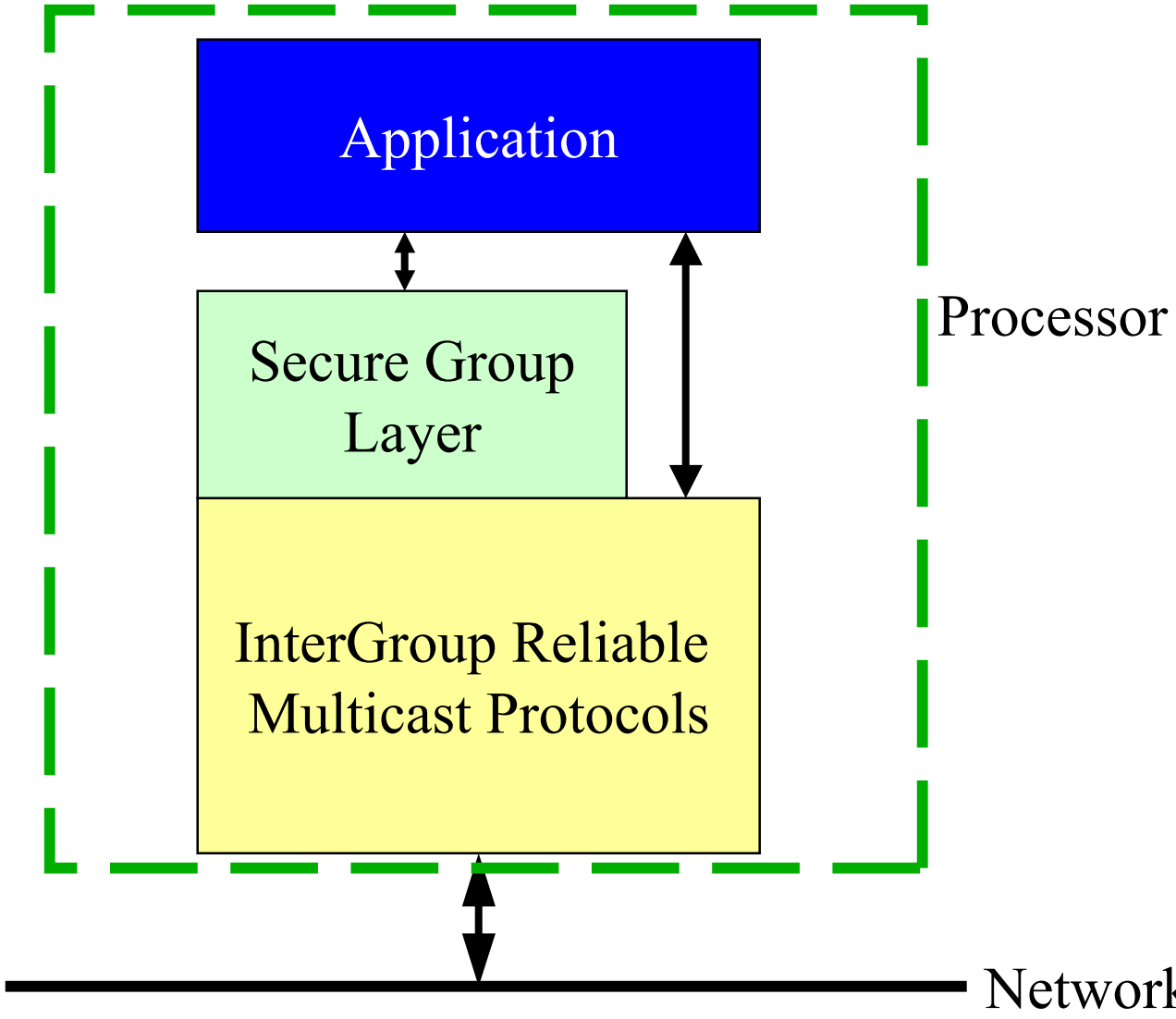
Secure and reliable multicast

- Provide efficient and reliable communication between participating sites
- Communication channel directly connecting the participants (no intermediary server)
- Support participants spread across the Internet
- Remove dependence on servers (support ad hoc formation of groups)
- Provide a secure group communication channel
  - — Authenticated members
  - — Authorization of members
  - — Data confidentiality
  - — Data integrity

Group Communication



Architecture



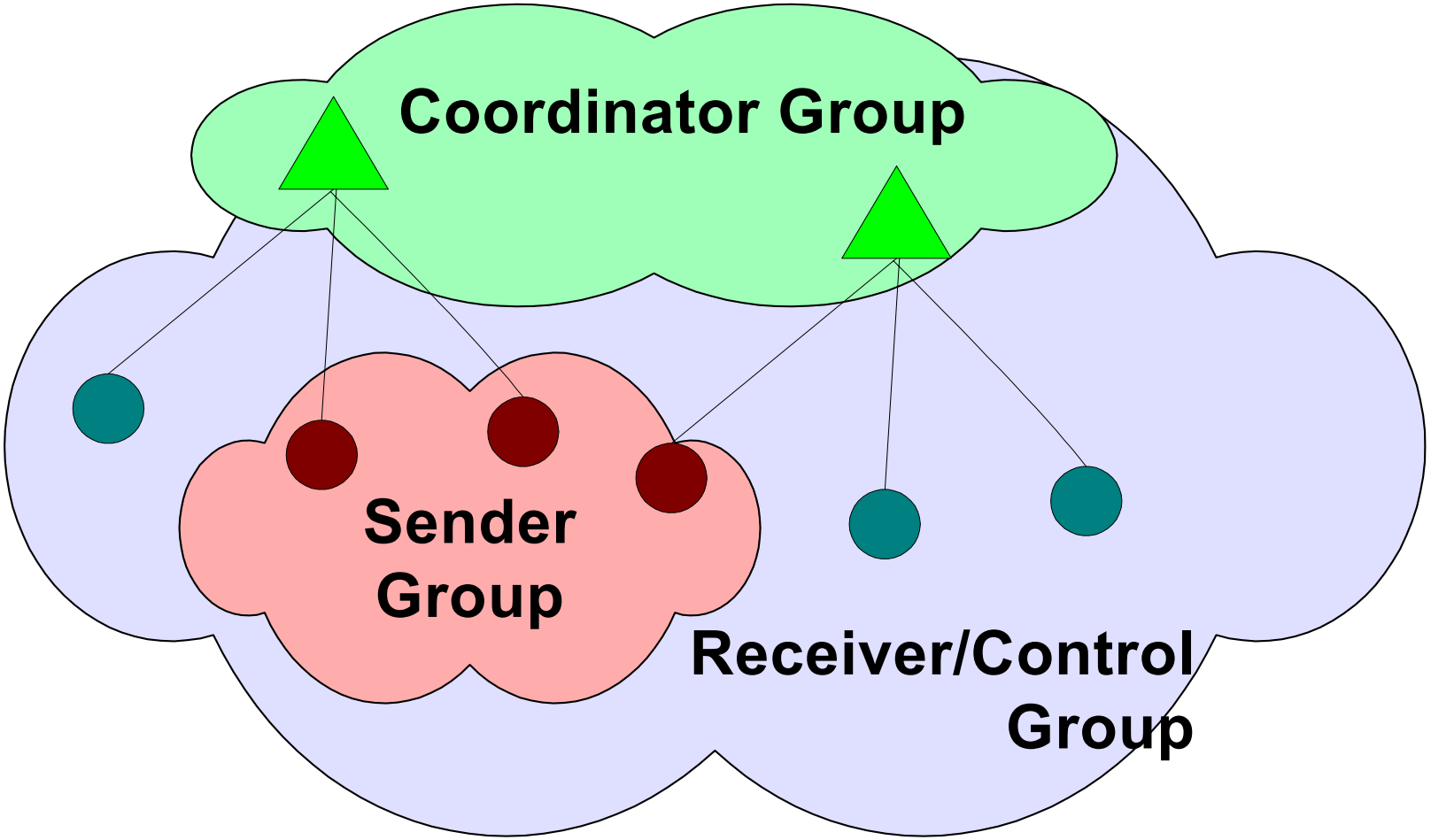
InterGroup Protocol

- All members of the group can send messages to the group
- All processes in the group receive the messages sent within the group
- Membership tracking with notification of membership changes
- Messages delivered at each member of the group in a consistent order
  - Timestamp order
  - Preserve causality
  - Membership changes delivered in order

InterGroup Protocol Scaling

- Split group into a sender and receiver group
  - — Sender group membership
    - processes are in the sender group only while transmitting messages
    - strictly maintained
    - very dynamic (small and fast)
  - — Receiver group membership
    - Hierarchical structure
    - not strictly maintained
    - used for retransmissions and garbage collection
    - proxy send for low frequency senders
- Flexible delivery options

InterGroup Schematic



InterGroup Design

- Automatically handles membership, message ordering and retransmission of missed messages
- Uses IP Multicast to transmit messages
- Core protocol implemented in Java (requires jdk v1.3 or higher)
- User interface
  - — Available in Java and soon in C++
  - — Usable as a library that connects via TCP to the InterGroup protocol on another machine (coming soon)
- Datagram type service (not streaming)

InterGroup Application Interface

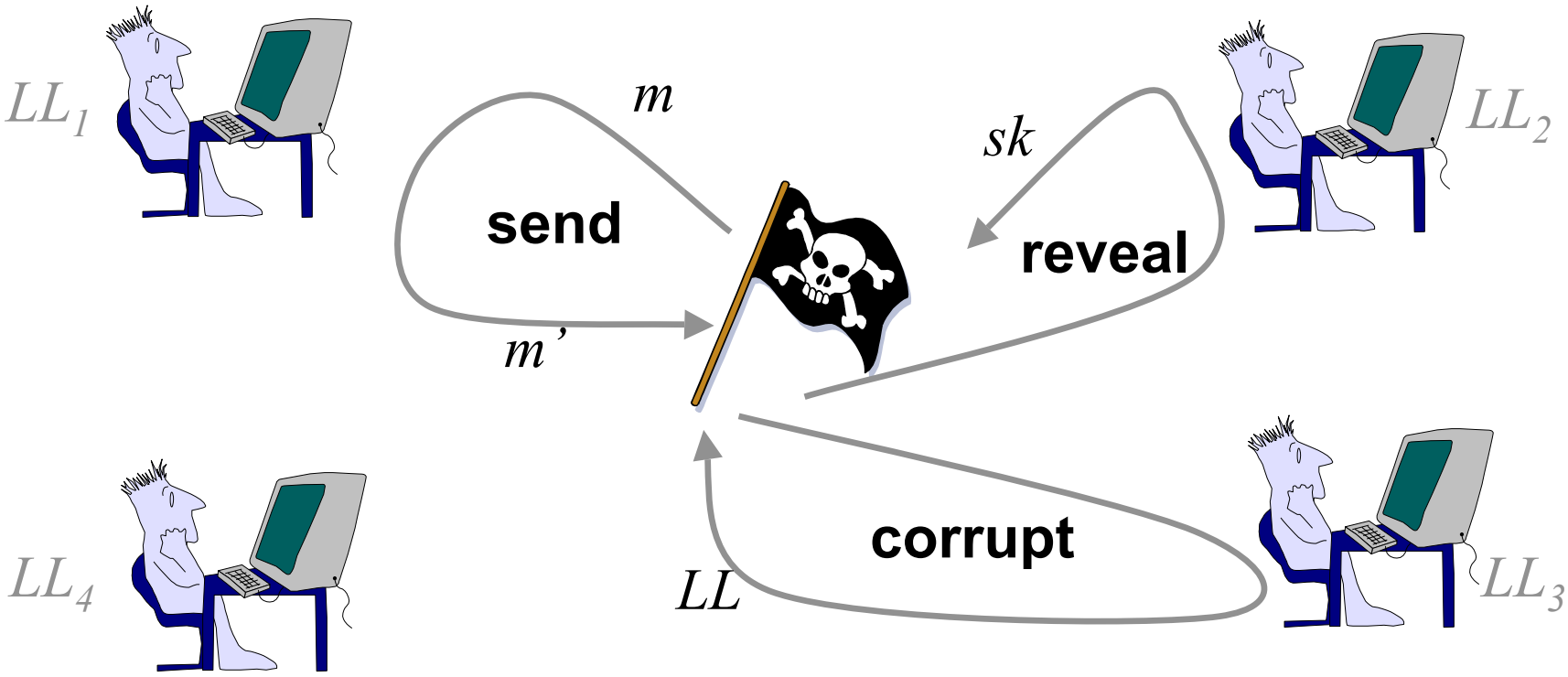
- User interface connection to InterGroup (Connection class)
  - SetName(“Deb Agarwal”)
  - Connect
  - Disconnect
- Group membership
  - SetName(<multicast address>, <port>)
  - Join
  - Leave
- Messages
  - Send(message)
  - OnData(group, sender, message)
  - OnMemb(group, membership)

Secure Group Layer

- Provides a secure channel for the group with properties similar to Secure Socket Layer (SSL)
- Authorization of group members using PKI (individually enforced)
- Key exchange
  - — Group Diffie-Hellman algorithms
  - — Based on provably secure crypto algorithms

Model for Proof of Security

- Adversary capabilities modelled via queries
  - send: send messages to instances
  - reveal: obtain an instance's session key
  - corrupt: obtain a player's long-lived key

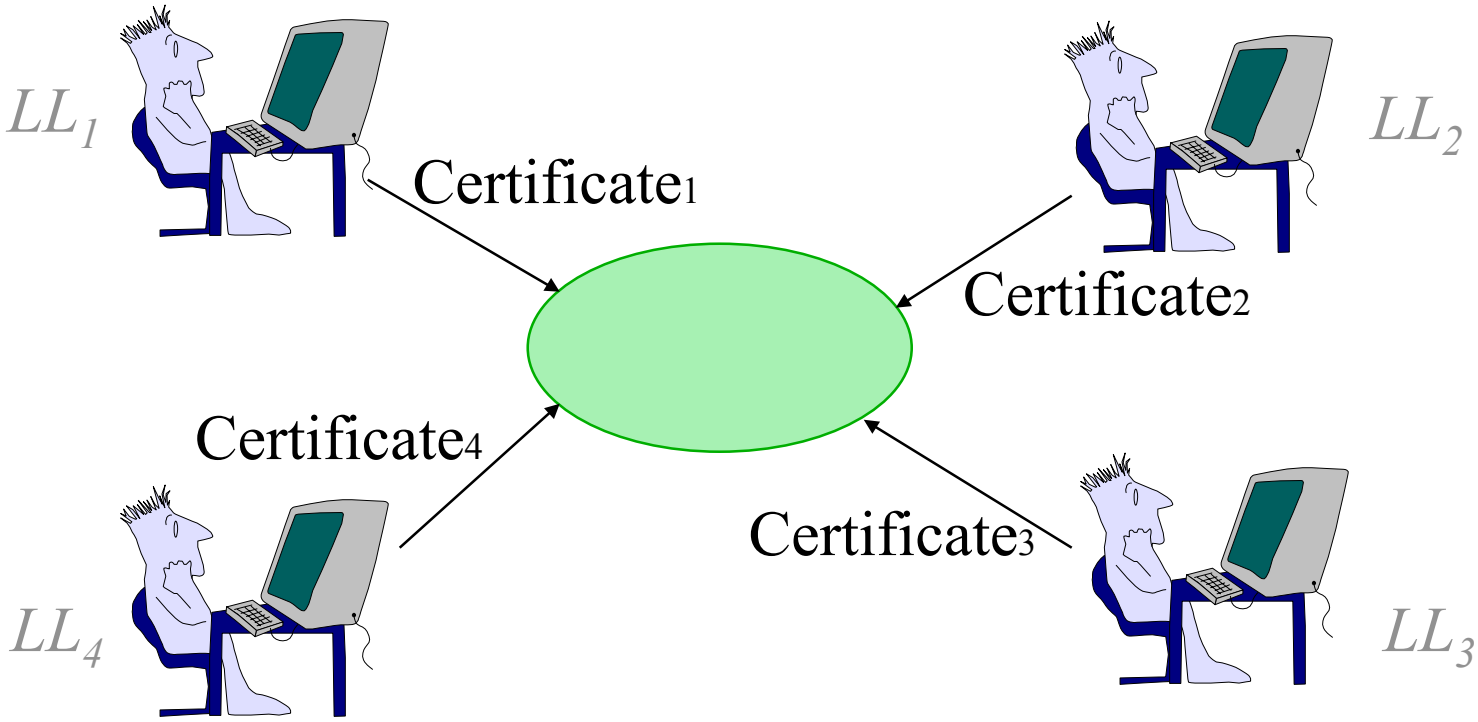


Security Goals

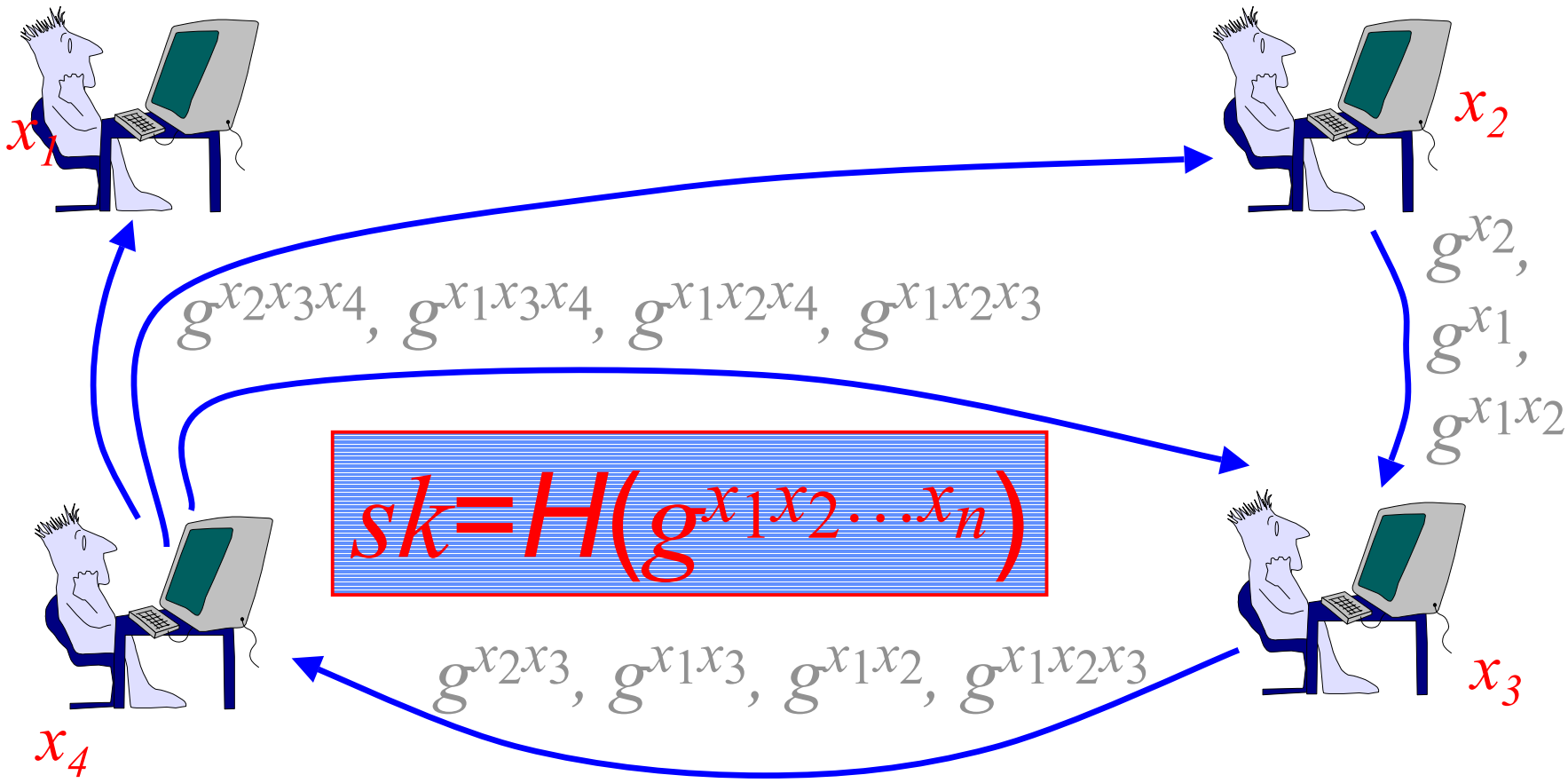
- Authenticated Key Exchange (AKE)
  - — Implicit Authentication:
    - Only the intended partners can compute the session key
  - — Semantic security:
    - A fresh session key is indistinguishable from a random string
- Mutual Authentication (MA)
  - — Each player is convinced of the identity of his partners

Building a Shared Key

- A set of n players which have many instances
- Each player holds a long-lived key



Key Exchange



Secure Group Design

- Group Diffie-Hellman used for the sender group
- Designing key distribution mechanisms for receivers
- Shared password-based key agreement also being designed
- Uses InterGroup for sending messages and notification of membership changes
  - — Verifies message ordering
  - — Determines membership
- Authorization interfaced to Akenti

Implementation

- Next alpha release of the InterGroup implementation expected in April 2002
  - Written in Java (clients available in Java and C++)
  - All processes in the sender group
  - Flow/congestion control very crude
- Secure Group Layer
  - Implementation underway
  - Completed proofs of security of distributed key agreement algorithms
  - Release not yet scheduled

Thoughts on Use of Group Communication in the Access Grid

- Coordination channel for venue control
- Window arrangement channel
- Securing the venue
  - — Generate session keys for use by the other AG tools
  - — Virtual venues
- Distributed PowerPoint coordination
- Distributed chat/Moo tool
- Voyager recording/playback
- Etc. . . .

URL: http://www-itg.lbl.gov/CIF/GroupComm/